Use Authentication Mechanisms, Where Appropriate, Correctly

William L. Fithen, Software Engineering Institute [vita[3]]

2005-10-03

Incorrectly using, or failing to use, authentication mechanisms can introduce vulnerability.

Description

The following are frequent design defects that produce vulnerable systems:

- Using no authentication when it is required.
- Failure to understand the limitations of the authentication scheme or mechanism. For example, HTTP basic authentication authenticates the user, not the server.
- Failure to separate authentication and authorization.
- Designing passwords that are inherently weak and disallowing passwords that are strong. For example, a system that supports only eight-character passwords composed of alphanumeric characters is a poor design (something that many web sites do) [VU#243592[10]].
- Using weak authentication based on untrustworthy attributes, such as network address information [VU#30308[11]].
- Disabling a subsystem's built-in access controls through identity sharing. This is a common practice in web sites that use back-end databases.
- Failing to propagate authentication across a multi-tier application.
- Designing a secure container for secrets and then exposing the secrets outside the container. This has occurred in several implementations of smart cards.

Applicable Context

Missing, incomplete, or incorrect application of an authentication mechanism.

Impacts Being Mitigated

- Impact #1:
    - **Minimally:** The least impact of this vulnerability is unauthenticated access to computing resources.
    - **Maximally:** The greatest impact of this vulnerability depends on the nature of the computing resources. In the worst case, these resources control access to other resources, in which case the result is a complete loss of integrity for the system.

[3] daisy:320 (Fithen, William L.)

[10] #refs

[11] #refs

Security Policies to be Preserved

- Policy #1
  - Access to computing resources is granted only to authentic individuals.

References

[VU#243592]	Cohen, Cory & Lanza, Jeffrey. *Vulnerability Note VU#243592: Alcatel ADSL modems provide EXPERT administrative account with an easily reversible encrypted password*. http://www.kb.cert.org/vuls/id/243592 (2001).
[VU#30308]	Rafail, Jason. *Vulnerability Note VU#30308: lpd hostname authentication bypassed with spoofed DNS*. http://www.kb.cert.org/vuls/id/30308 (2001).

SEI Copyright

Fields

Name	Value
Copyright Holder	SEI

Fields

Name	Value
is-content-area-overview	false

[1] http://www.sei.cmu.edu/about/legal-permissions.html

Content Areas	Knowledge/Guidelines
SDLC Relevance	Implementation
Workflow State	Publishable